Solutions 2

#1 The polynomial $x^5 + x^3 + 2x + 2$ in $\mathbf{Z}/3[x]$ has a repeated factor. Find it.

The derivative is $5x^4 + 3x^2 + 2 = 2x^4 + 2$. We could replace this by the *monic* version of the polynomial, which would make life a little simpler, but we won't here, just to show that it's not necessary. Note that $2^{-1} = 2 \bmod 3$. The polynomial does not fall into the special case, so we should use the Euclidean Algorithm to compute the gcd of it and its derivative: (without showing all the long divisions...)

$$\begin{array}{ccccc} (x^5 + x^3 + 2x + 2) & - & (2x)(2x^4 + 2) & = & x^3 + x + 2 \\ (2x^4 + 2) & - & (2x)(x^3 + x + 2) & = & x^2 + 2x + 2 \\ (x^3 + x + 2) & - & (x + 1)(x^2 + x + 2) = 0 & & \end{array}$$

Thus, the gcd is $x^2 + 2x + 2$. We test the latter for irreducibility by testing for roots to the equation $x^2 + 2x + 2 = 0$ in $\mathbf{Z}/3$, since if it factored it would have to have a linear factor (being just quadratic). But $0^2 + 2 \cdot 0 + 2 = 2 \neq 0$, $1^2 + 2 \cdot 1 + 2 = 2 \neq 0$, $2^2 + 2 \cdot 2 + 2 = 8 = 2 \neq 0$, so there are no roots, and no linear factors. Thus, by the theorem, $(x^2 + 2x + 2)^2$ divides the original polynomial.

#2 Compute the 18^{th} cyclotomic polynomial.

Use the recursive definition (and subsequently, slightly clever grouping):

$$\varphi_{18} = \frac{x^{18} - 1}{\prod_{1 \leq d < 18, d | 18} \varphi_d(x)} = \frac{x^{18} - 1}{\varphi_1 \varphi_2 \varphi_3 \varphi_6 \varphi_9} = \frac{x^{18} - 1}{\varphi_2 \varphi_6 \ (x^9 - 1)}$$

since $\varphi_9 = \varphi_1 \varphi_3 \varphi_9$. Invoking the basic algebra identities, we have

$$\varphi_{18} = \frac{x^9 + 1}{\varphi_6 \, \varphi_2}$$

Computing separately, $\varphi_2 = (x^2 - 1)/\varphi_1 = x + 1$, and slightly more complicately

$$\varphi_2(x)\varphi_6(x) = \varphi_2(x)(x^6 - 1)/\varphi_1(x)\varphi_2(x)\varphi_3(x) = \varphi_2(x)(x^6 - 1)/\varphi_2(x) \, (x^3 - 1)$$

$$= (x^6 - 1)/(x^3 - 1) = x^3 + 1$$

Thus,

$$\varphi_{18}(x) = \frac{x^9 + 1}{\varphi_6 \, \varphi_2} = \frac{x^9 + 1}{x^3 + 1} = x^6 - x^3 + 1$$